This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-64. (Cancelled)

65. A method for mobile internet protocol (IP) route optimization comprising:

forwarding a datagram from a correspondent node to a mobile node using a shortest path between the mobile node and the correspondent node, wherein the mobile node is in a mobile IP visiting network having a mobile IP protocol, and wherein the correspondent node is unaware of the mobile IP protocol.

66. The method of claim 65, further comprising:

registering the mobile node with the mobile IP visiting network; and

adding a route entry to a routing table in a mobile IP foreign agent.

67. The method of claim 66, further comprising:

removing the route entry from the routing table when the registered mobile node de-registers or times out.

68. The method of claim 66, wherein the route entry comprises:

a destination address comprising an address for a home network of the mobile node;

a nexthop value comprising a local interface to which the mobile node is attached; and

a routing cost comprising a value lower than all other routes available to the mobile node.

69. The method of claim 68, further comprising:

routing the datagram based on the destination address.

70. The method of claim 69, wherein routing the datagram comprises using a routing protocol comprising one of Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

71. The method of claim 66, wherein the route entry comprises:

a source address comprising an address of the mobile node;

a destination address comprising a set of subnetworks in a vicinity of the mobile IP foreign agent; and

a nexthop value comprising a local interface of the mobile IP foreign agent.

72. The method of claim 71, wherein routing the datagram comprises performing source-restricted destination address routing.

73. The method of claim 72, wherein a route of the datagram is not propagated to a router using a routing protocol.

74. The method of claim 66, further comprising:

performing dynamic Network Address Translation (NAT) for a second datagram sent from the mobile node to a second correspondent node, wherein the second correspondent node is part of the mobile IP visiting network.

75. The method of claim 74, further comprising:

indexing a state in a state table using a mobile node home network address and a link layer address.

76. The method of claim 75, further comprising:

accepting the state from the state table when the mobile node has a valid registration.

77. The method of claim 75, further comprising:

denying the state from the state table when the mobile node does not have a valid registration.

78. The method of claim 75, wherein indexing the state in the state table comprises indexing by the link layer type with which the mobile node attaches to the mobile IP foreign agent.

79. The method of claim 66, further comprising:

distributing static routes and filters for the mobile node to the mobile IP foreign agent.

80. The method of claim 79, wherein distributing static routes and filters occurs at a time of configuration.

81. The method of claim 79, wherein distributing static routes and filters occurs at a time of registering the mobile node.

82. The method of claim 79, wherein distributing static routes and filters occurs as part of a DIAMETER response from a home agent to the foreign agent.

83. The method of claim 79, further comprising:

tying the filters to a mobile node home network address and a home agent address.

84. The method of claim 83, further comprising:

applying the filters to traffic sent from the mobile node on a local subnet when the mobile node has a valid registration.

85. The method of claim 83, further comprising:

blocking the filters when the mobile node does not have a valid registration.

86. The method of claim 66, further comprising:

allocating a care-of address to the mobile node using a dynamic host configuration procedure.

87. The method of claim 86, further comprising:

applying the care-of address as a source address to a virtual interface adapter in the mobile node; and

using the virtual interface adapter for traffic to destinations within the mobile IP visiting network.

88. The method of claim 87, further comprising:

enabling the virtual interface adapter at a time of registering the mobile node.

89. The method of claim 87, further comprising:

disabling the virtual interface adapter at one of a time when a registration of the mobile node is no longer valid, and a time when the mobile node moves to a new mobile IP visiting network.

90. The method of claim 81, further comprising:

giving a home agent tunnel a lower routing cost as nexthop compared to local IP connectivity for the static routes.

91. The method of claim 90, wherein registering the mobile node with the mobile IP visiting network involves a dynamic host configuration procedure in a home network.

92. The method of claim 91, wherein distributing the static routes comprises including the static routes as an extension in a mobile IP registration reply message as part of the dynamic host configuration procedure.

93. The method of claim 92, further comprising:

giving local IP connectivity a lower routing cost as nexthop compared to a home agent tunnel for static routes distributed as part of the dynamic host configuration procedure.

94. The method of claim 86, further comprising:

applying filter rules at the mobile node for traffic being sent and received with local IP connectivity and a home agent tunnel respectively.

95. The method of claim 94, wherein the filter rules are distributed to the mobile node at a time of configuration.

96. The method of claim 94, wherein the filter rules are distributed to the mobile node at a time of registering the mobile node.

97. The method of claim 96, wherein the filter rules are distributed as an extension in a mobile IP registration reply message.

98. The method of claim 66, further comprising:

applying a selective reverse tunneling scheme between a home agent tunnel and local IP connectivity using a routing prefix and a routing cost.

99. The method of claim 98, further comprising:

giving a lower routing cost to a home agent tunnel route as nexthop compared to local IP connectivity when private address realms for the visiting network and the home network overlap.

100. The method of claim 98, further comprising:

giving a lower routing cost to a home agent tunnel route as nexthop compared to local IP connectivity for a route to the Internet.

101. The method of claim 98, further comprising:

giving a lower routing cost to local IP connectivity as nexthop compared to a home agent tunnel route for a route to a same subnetwork as the mobile node.

102. The method of claim 98, further comprising:

giving a lower routing cost to a home agent tunnel route as nexthop compared to local IP connectivity for a route to a home network.

103. The method of claim 66, further comprising:

hosting a home network of the mobile node using a plurality of home agents, the home agents having a same home agent IP address.

104. The method of claim 103, further comprising:

dispatching a plurality of messages among the home agents using a load balancer.

105. The method of claim 104, further comprising:

retrieving data about a mobile node user at a time of registering the mobile node from at least one of a common AAA server, and an LDAP directory.

106. The method of claim 103, further comprising:

sending a message from a one of the plurality of home agents to a care-of address using a direct server return method.

107. The method of claim 106, further comprising:

sending a routing update related to availability of the mobile node to a router.

108. The method of claim 104, further comprising:

sending an ICMP destination unreachable message from the load balancer to a tunnel decapsulator when an assigned home agent fails; and

reporting a tunnel soft state as network unreachable when a foreign agent is the tunnel decapsulator.

109. The method of claim 108, further comprising:

sending a new registration to the same home agent IP address upon receipt of the ICMP destination unreachable message.

110. The method of claim 109, further comprising:

confirming that a one of the plurality of home agents is alive before allocating a registration request to the one of the plurality of home agents.

111. The method of claim 109, further comprising:

allocating a new home agent for the mobile node.

112. The method of claim 109, wherein a first home agent acts as a primary agent and a second home agent acts as a secondary agent for the same home agent IP address.

113. The method of claim 66, further comprising:

using a care-of address which resides behind a network address translation;

rejecting a first registration request from the mobile node when a source address in a header of the first registration request is different from a care-of address within the first registration request; and

sending a challenge.

114. The method of claim 113, further comprising:

responding to the challenge with a second registration request.

115. The method of claim 114, further comprising:

using the source address of a registration request as the destination address for encapsulated datagrams sent to the care-of address.

116. The method of claim 115, further comprising:

using a source address of a reply to a registration request as the source address for encapsulated datagrams sent to a home agent.

117. The method of claim 113, further comprising:

performing address masquerading using a port translation; and

tunneling a payload datagram from the care-of address to a home agent using UDP between an inner IP header and an outer IP header.

118. The method of claim 66, further comprising:

establishing a plurality of mobile IP security associations between the mobile node, a home agent, and a foreign agent using public key certificates; and

signing the public key certificates using a mobile service manager.

119. The method of claim 118, further comprising:

configuring the foreign agent with one of the public key certificates and a public key certificate of the mobile service manager;

configuring the home agent with one of the public key certificates and the public key certificate of the mobile service manager; and

configuring the mobile node with one of the public key certificates, the public key certificate of the mobile service manager, and the public key certificate of the home agent.

120. The method of claim 119, further comprising:

including the public key certificate of the mobile node as a mobile IP extension in a registration request message;

including the public key certificate of the foreign agent as a mobile IP extension in the registration request message; and

including the public key certificate of the home agent and the public key certificate of the foreign agent in a registration reply message.

121. The method of claim 120, further comprising:

verifying a signature of one of the public key certificates using the mobile service manager.

122. The method of claim 121, further comprising:

matching a received certificate to a certificate revocation list provided by the mobile service manager at a time of configuration.

123. The method of claim 122, further comprising:

validating the public key certificate of the foreign agent on behalf of the mobile node; and

sending a signed version of the public key certificate of the foreign agent to the mobile node in a registration reply message.

124. The method of claim 122, further comprising:

applying a public key of the received certificate to an authenticator in a mobile IP authentication extension.

125. The method of claim 124, further comprising:

applying a public key of the public key certificate of the foreign agent to the authenticator in the mobile IP authentication extension.

126. The method of claim 124, further comprising:

establishing a Security Parameter Index (SPI) equal to a predetermined integer larger than 255 between a pair of nodes when authentication is successful.

127. The method of claim 126, further comprising:

establishing one of IP security, and transport layer security using a same X.509 certificate among the mobile node, the foreign agent, and the home agent.

128. The method of claim 125, further comprising:

accessing one or more servers in a home network and a visiting network using respectively the home agent and foreign agent as security proxies.